A Merchant Announces A Data Breach; What Should You Do?

Recently both global hotel chain Marriott International (500 million) and Quora (100 million), one of the largest Q&A internet portals, announced security breaches compromised their data.

So how should you respond?

For approximately 327 million Marriott guests the information included some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the data also included encrypted payment card numbers and expiration dates.

The personal user data compromised in the Quora breach included, account information (names, emails, hashed passwords, and data imported from linked social networks like Twitter and Facebook); public actions (questions, answers, comments, and upvotes); and non-public content (answer requests, downvotes, and direct messages).

So what can users do to protect their personal information?

1. **Get back into your account.** The first important step is to log into the account and change the password immediately. "It shouldn't be 'password' or 'imthekingoftheworld.'" Your password needs to be strong. Try this trick: think of a statement, for example, "I love to go for a walk every evening." Then, turn it into 1I2g4awEVe (replacing I with 1, to with 2, for with 4, and every with EV). If possible, use two-step authentication and get a password manager. Most importantly, never reuse the same password for all accounts.
2. **Take care of other accounts.** For those, that use the same or similar password for more than one account, change it on all other key platforms and accounts immediately. That includes email, Facebook, Amazon, Twitter, LinkedIn, and others. "Even though hackers, most probably, got hold of your hashed password, there's still a chance they can decrypt it and get the real password." Check haveibeenpwned.com for any compromised accounts.
3. **Update settings and available data.** Go through the privacy settings and data provided on the breached platform and all the other important platforms used. Make sure to share only the required information and remove what's not necessary. This way, even if your account gets hacked, it will be of less value for hackers. Common advice is to share as little as possible online; and change your account settings from 'Public' to 'Private.'
4. **Revoke access to third-party apps.** "In Quora's case, for the user convenience, there was a possibility to import some data from linked social networks like Twitter and Facebook. And it seems that hackers got hold of this information as well." Check, whether the permissions on access to those accounts. Revoke access to applications that are no longer in use, as well as suspicious ones.
5. **Beware of phishing scams.** Since hackers may have detailed profile information of 100 million users on Quora, we are likely to see more personalized and sophisticated phishing scams soon. "Phishing scams are very effective, as criminals usually use a piece of real private information." Users should be careful if they received seemingly legitimate, personalized messages from financial institutions or any other familiar organizations. "That is especially valid if they ask for more personal details, fund transfers or to click on any link."

Information provided by Credit Union Times, 12/6/2018.